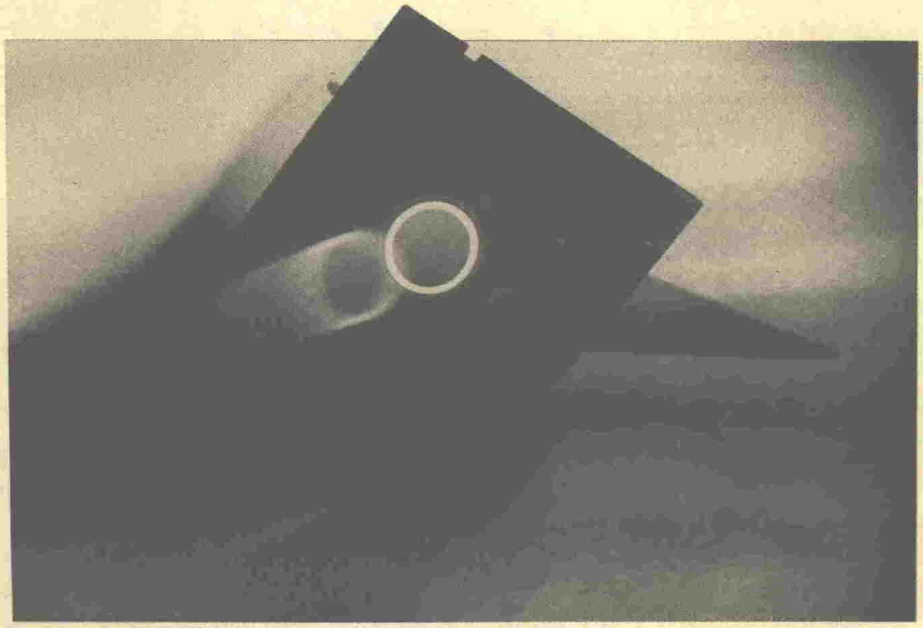
โรคไวรัสในแผ่นดิสค์ (IBM)



ชาญชัย สัจจอิสริยวุฒิ
สุรเมธ สัจจอิสริยวุฒิ

Virus คืออะไร

Virus คือ โปรแกรมที่ถูกเขียนขึ้นมาเพื่อทำลายข้อมูล โดยสามารถติดจากแผ่นดิสค์หนึ่งไปยังอีกแผ่นหนึ่งได้ เหมือนกับการติดเชื้อของมนุษย์ โดยที่ตัวโปรแกรมไวรัสจะไปแอบซ่อนอยู่ในแผ่นดิสค์และจะค่อย ๆ ทำลายข้อมูลและรบกวนระบบการทำงานของดิสค์-ไดรฟ์เหมือนเช่นคนที่ป่วยติดเชื้อจะมีอาการผิดปกติจากเดิม และทำงานได้ไม่เหมือนเดิม

ประมาณต้นปีมีข่าวว่า มีการพบโปรแกรมไวรัส ซึ่งสามารถติดต่อได้และมันจะแอบทำลายข้อมูลโดยไม่รู้ตัว และมีการระบาดเข้ามาในเมืองไทย ผู้เขียนจึงได้ทำการค้นหาว่าแผ่นดิสค์ของผู้เขียนเองมีไวรัสแอบซ่อนอยู่หรือไม่ ถ้ามีและหากข้อมูลถูกทำลายไป ผู้เขียนคงต้องใช้เวลานานทีเดียวในการหาโปร-แกรมและทำการซ่อมแซมข้อมูลให้กลับคืนสู่สภาพเดิม แต่ปรากฏว่าไม่พบว่ามีไวรัส และทางผู้เขียนเองได้พยายามค้นหาตัวโปรแกรมไวรัสเพื่อทำการทดสอบว่าหน้าตาของมันเป็นอย่างไร แต่หาไม่พบเลยจนเลิกสนใจไป แต่เมื่อไม่นานมานี้ผู้เขียนได้มีโอกาสพบโปรแกรมไวรัสจากรุ่นน้องของผู้เขียนคนหนึ่ง โดยพบว่ามีการติดไวรัสบนดิสค์ถึง 2 กล่องทีเดียว แม้แต่โปรแกรมเกมก็ติดไวรัสไปด้วย ผู้เขียนจึงได้นำตัวอย่างของไวรัสมาทำการเพาะไว้หลายแผ่น และทดลองให้เกิดการแพร่ของไวรัสให้มันติดต่อกันไปติดต่อกันมา จนพอมีความเข้าใจตัวไวรัสบ้าง จึงได้ทำการเขียนโปรแกรมสำหรับค้นหาว่าแผ่นดิสค์แผ่นใดที่มีไวรัสแอบซ่อนอยู่ และสามารถทำการรักษาให้หายเป็นปกติ และผู้เขียนได้ให้ชื่อโปรแกรมนี้ว่า **ศิริราช (Siriraj)** และต่อไปเราจะกล่าวถึงไวรัสในดิสค์อย่างละเอียด

การติดต่อ

จากการทดลองพบว่าการติดต่อของไวรัส เริ่มจากการบูตด้วยแผ่นที่มีไวรัส (ทั้งที่มีดอสหรือไม่มีดอสก็ตาม) ตัวไวรัสจะไปแอบในหน่วยความจำของเครื่องและพร้อมที่จะติดต่อไปยังแผ่นอื่น เมื่อมีการเรียกใช้งานดิสค์ เช่น copy, dir, ren, format ฯลฯ (รวมทั้งการเรียกใช้งานดิสค์จากโปรแกรมต่าง ๆ ด้วย)

อาการเมื่อติดไวรัส

1. เมื่อทำการเริ่มบูตแผ่นที่มีไวรัส จะพบว่าใช้เวลาในการเริ่มทำงานมากกว่าปกติ เพราะต้องเอาโปรแกรมไวรัสเข้าไปไว้ในหน่วยความจำก่อนที่จะเริ่มทำงานตามปกติ

2. เมื่อไวรัสจะติดต่อไปยังแผ่นดิสค์ใด ในการทำงานนั้น ๆ จะใช้เวลาในการทำงานมากกว่าปกติ เช่นในการก๊อบปี้จะใช้เวลานานมากขึ้น เพราะไวรัสจะต้องใช้เวลาในการตรวจสอบและแพร่ก่อนที่จะทำการก๊อบปี้ต่อไปตามปกติ

3. เมื่อทำการ dir จะพบว่า DISK VOLUME จะเปลี่ยนไปจากเดิมเป็น (C) Brain และจะพบว่าจำนวนไบต์

ที่ว่างอยู่ของแผ่นที่ติดไวรัส จะมีขนาดลดลงจากเดิมประมาณ 3 กิโลไบต์

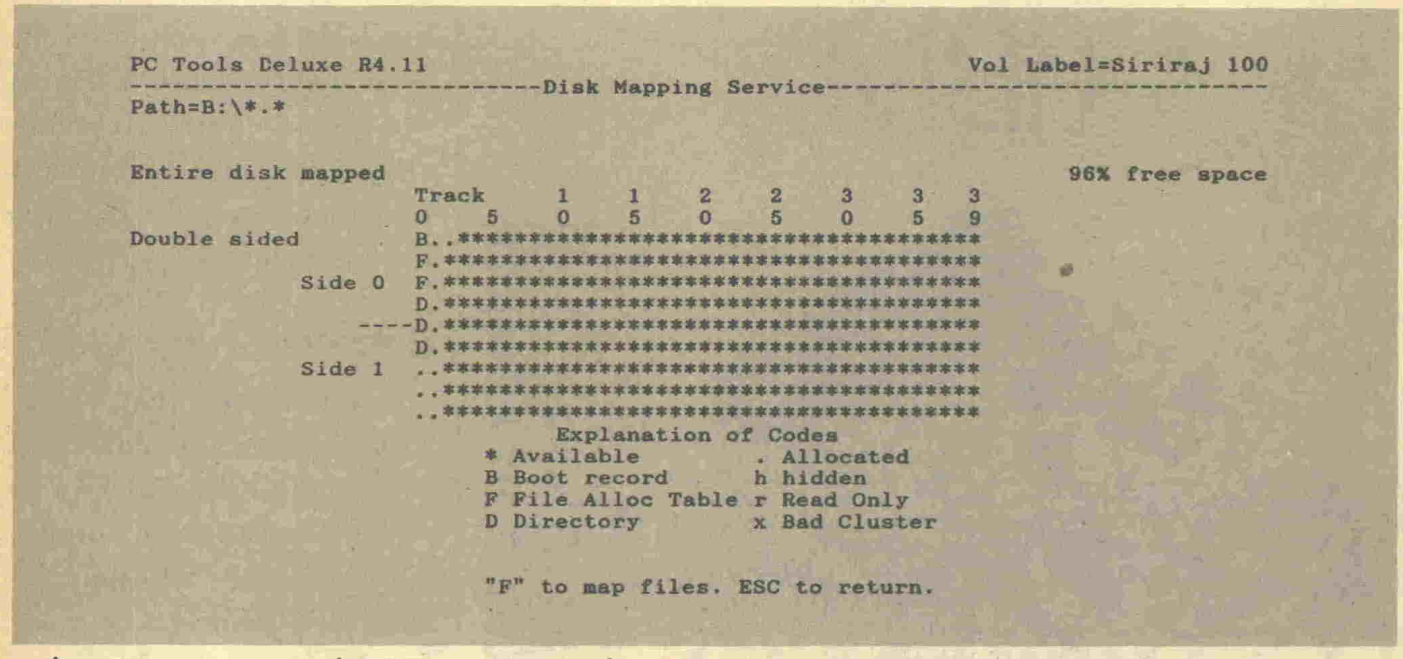
4. เมื่อใช้ไปนาน ๆ จะมีอาการของโปรแกรมที่เคยใช้งานได้ จะใช้ไม่ได้ หรือมีอาการรวนเพราะถูกทำลาย

5. เมื่อใช้ View/Edit ของ PC-TOOLS หรือ EDIT ของ NORTON UTILITY มาดูที่ Track 0, Sector 1, Side 0 (BOOT SECTOR) จะพบว่ามีการเปลี่ยนไปจากปกติ เป็นลักษณะดังรูปที่ 3 เสมอ

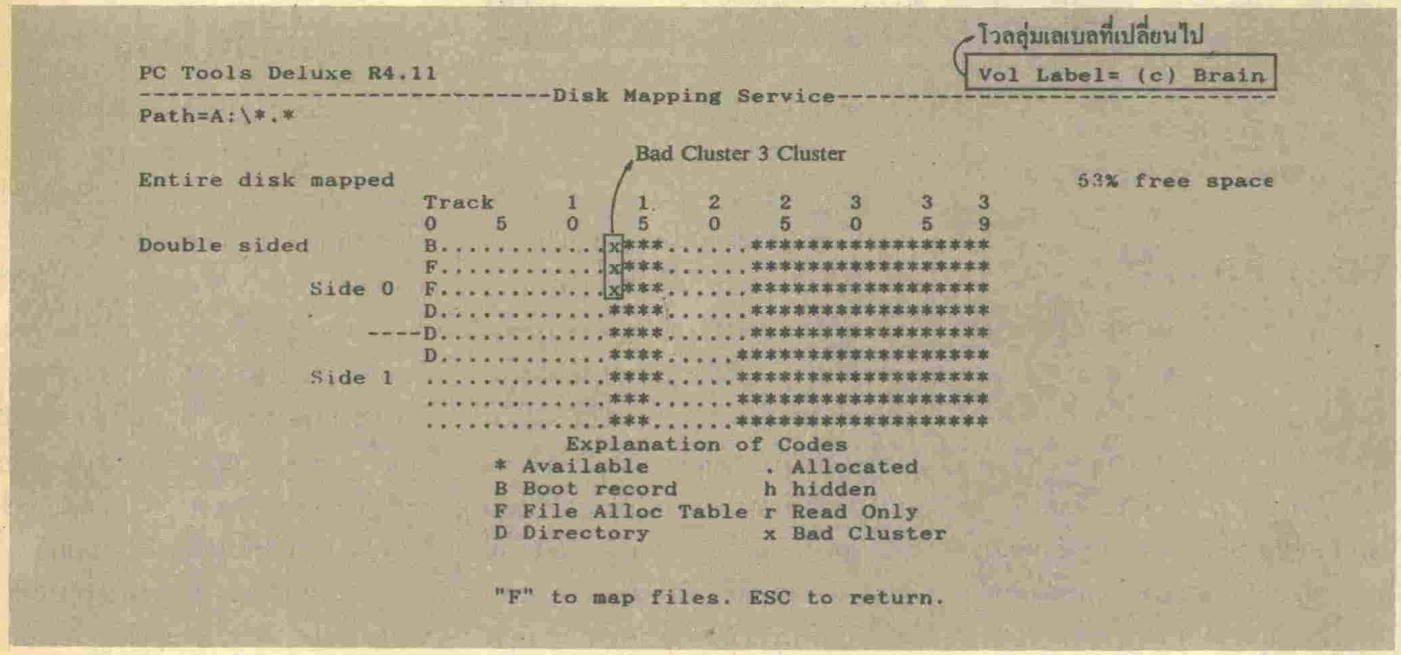
คุณสมบัติพิเศษของไวรัส

– เมื่อมีการบูตด้วยแผ่นที่มีไวรัสอยู่ และไวรัสได้ไปแอบซ่อนในหน่วยความจำแล้ว จะไม่สามารถตรวจพบไวรัสได้ ด้วยวิธีการดังข้อ 5

– มีบางครั้งเมื่อติดไวรัสมา เมื่อทำการไดเรคทอรีแล้ว DISK VOLUME อาจจะไม่เปลี่ยนเป็น (c) Brain ดังนั้นวิธีการที่ตรวจหาไวรัสที่ดีที่สุด คือ การใช้โปรแกรมในการตรวจและรักษาไวรัสโดยตรง เช่น โปรแกรม ศิริราช (Siriraj), Un-Virus ฯลฯ หรือใช้ PCTOOLS,



รูปที่ 1 แผนผังของแผ่นดิสค์ที่ฟอร์แมตมาใหม่ ๆ เมื่อเรียกดูโดยใช้ฟังก์ชัน Mapping ของ PC Tools R 4.11



รูปที่ 2 แผ่นดิสค์ที่ติดไวรัสแล้วสังเกตมี Bad Cluster 3 Cluster

NORTON UTILITY เข้าไปดูที่ Boot Sector ดังกล่าวมาข้างต้น

– ไวรัสจะไม่ติดในแผ่นที่เป็นแบบ 8 เซกเตอร์ เช่น MS-DOS Version 1.00

– ไวรัสจะไม่สามารถติดต่อลงแผ่นที่มีการติด Write Protect Tab

– เมื่อตรวจหา Bad Cluster จะพบว่ามี Bad Cluster เพิ่มขึ้นจากเดิม 3 คลัสเตอร์ ซึ่งถูกนำไปใช้เก็บตัวโปรแกรมไวรัส

การป้องกันการแพร่ของไวรัส

– ต้องตรวจสอบแผ่นว่ามีไวรัสหรือไม่อย่างสม่ำเสมอด้วยโปรแกรมตรวจหาไวรัส โดยเฉพาะในแผ่นที่เพิ่งก๊อบปี้มาใหม่

– เมื่อพบต้องรีบทำการกำจัดไวรัสทิ้งโดยทันที ด้วยโปรแกรมตรวจและรักษาไวรัส

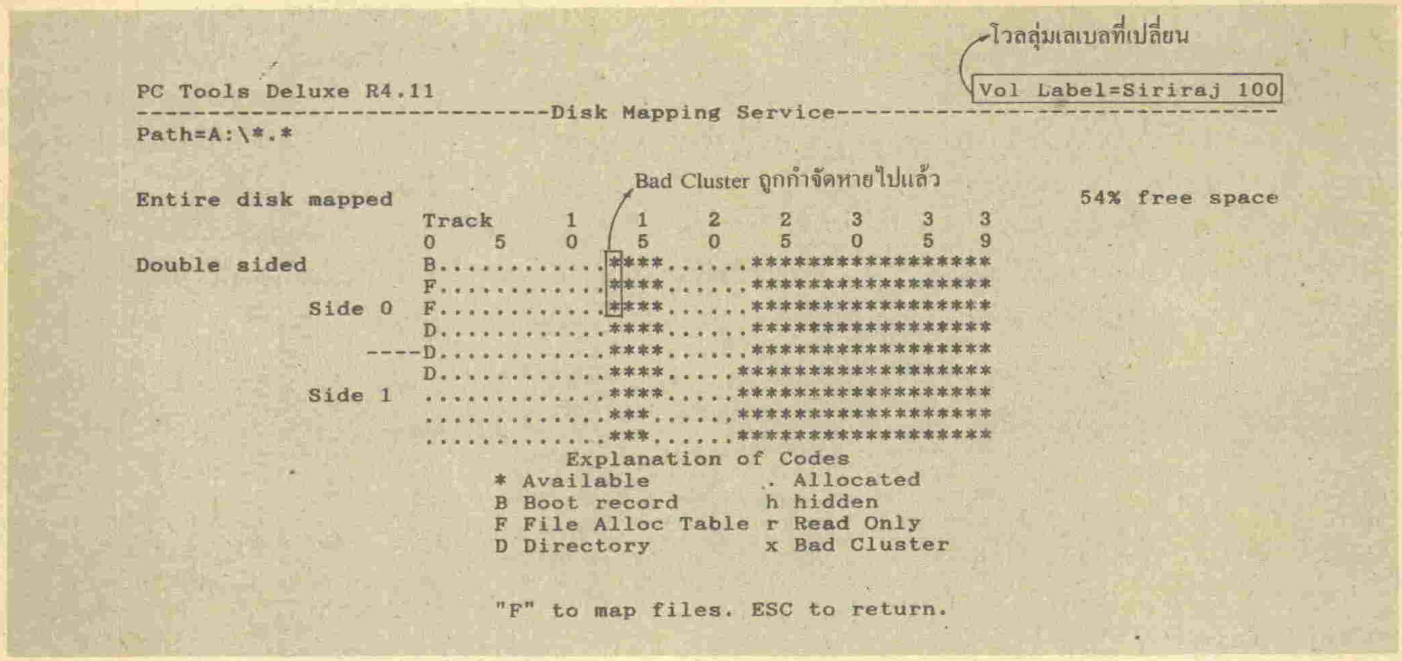
– แผ่นข้อมูลที่สำคัญ ควรมีการสำรอง และติด Write Protect Tab ไว้เสมอ

```
PC Tools Deluxe R4.11
------------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 00000, System BOOT

Displacement ----------------- Hex codes--------------------     ASCII value
 0000(0000)  FA E9 4A 01 34 12 00 01 0D 00 01 00 00 00 00 00    J 4
 0016(0010)  57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20   Welcome to the
 0032(0020)  44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20   Dungeon
 0048(0030)  28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26   (c) 1986 Brain &
 0064(0040)  20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74    Amjads (pvt) Lt
 0080(0050)  64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20   d   VIRUS_SHOE
 0096(0060)  52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20   RECORD    v9.0
 0112(0070)  44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65   Dedicated to the
 0128(0080)  20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65    dynamic memorie
 0144(0090)  73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66   s of millions of
 0160(00A0)  20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E    virus who are n
 0176(00B0)  6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73   o longer with us
 0192(00C0)  20 74 6F 64 61 79 2C 2D 20 54 68 61 6E 6B 73 20    today - Thanks
 0208(00D0)  47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20   GOODNESS!!
 0224(00E0)  20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65    BEWARE OF THE e
 0240(00F0)  72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69   r..VIRUS  : \thi

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

รูปที่ 3 เมื่อใช้ฟังก์ชัน View/Edit ของ PC Tools ดูที่แทร็คที่ 0, เซกเตอร์ที่ 1, ด้านที่ 0 (บูตเซกเตอร์) จะพบว่ามีข้อความเกี่ยวกับไวรัสเกิดขึ้น

```
A:\>siriraj
   SIRIRAJ.... program to diagnose and treat viral diskette.
       By  Ext.Chanchai sajjaisariyavut.  Siriraj' 94.
                Suramet  sajjaisariyavut.  Applied Physics. KMITL

  Do you want to Search for Virus ? y

 Dangerous! Detected virus in drive A:!
Do you want to KILL virus in drive A ? (Y/N)
Wait a few second... Infected Disk is still under treatment.

 infected organ.
 T13 Sec1 side0
Ready! Now diskette in drive A: has a good health.


Do you want to Search for Virus ? y
Diskette in drive A: is quite healthy.


Do you want to Search for Virus ? n
O.K. QUIT.
A:\>
```

รูปที่ 4 การใช้งานโปรแกรม SIRIRAJ กำจัดไวรัสบนแผ่นดิสค์ที่ติดไวรัส



รูปที่ 5 แผ่นไวรัสที่ผ่านขั้นตอนการกำจัดไวรัสแล้วจะมีแผนผังของดิสค์เปลี่ยนไป

รูปที่ 7
โปรแกรม SIRIRAJ
เขียนด้วยภาษาซี
ใช้โปรแกรม
TURBO C 1.0

```
/*
   PROGRAM..... SIRIRAJ
   Release..... 1.0
   Perpurse.... to treat the viral diskette
   Language.... TURBO-C Version 1.00
   Last update. May 4,1988
   Time........ 02:35:00
   Programmer.. LOUIS & LEK
   Copyright... May (C) 1988
   Note........ This program is PUBLIC DOMAIN not for Sale
                If you found for sale, Please contact ous. Thankyou
*/
#include (dos.h)
#include (ctype.h)
main()
[ unsigned char data[1024];
  int a,sector,b,c;
  printf("   SIRIRAJ.... program to diagnose and treat viral diskette.\n"
         "         By  Ext.Chanchai sajjaisariyavut.  Siriraj' 94.\n"
         "             Suramet  sajjaisariyavut.  Applied Physics. KMITL\n");
  printf("Do you want to Search for Virus ? ");
  while ( (a=toupper(getche())) == 'Y' )
  [
    a = absread(0,1,0,data);
    while ( a == -1 )
       [
        printf("\nDrive does not Ready! Please check your drive A: \n");
        getch();
        a = absread(0,1,0,data);
       }
    if ((data[0] == 0xfa) && (data[1] == 0xe9) && (data[2] == 0x4a) && (data[3] == 0x01) && (data[4] == 0x34) && (data[5] == 0x12))
     [ printf("\n Dangerous! Detected virus in drive A:!\n");
       printf("Do you want to KILL virus in drive A ? (Y/N)");
       if ((a=toupper(getch())) == 'Y')
          [
           printf("\nWait a few second... Infected Disk is still under treatment.\n");
           sector = (data[8]*18)+data[7]+(data[6]*9)-1;
           printf("\n infected organ.");
           printf("\n T%d Sec%d side%d",data[8],data[7],data[6]);
           a = absread(0,1,sector,data);.
           abswrite(0,1,0,data);
           absread(0,2,1,data);
           a =(3*(sector-12)/4)+3;
           b= sector%4;
           if( b == 0)
```

```
PC Tools Deluxe R4.11
------------------------------Disk View/Edit Service-----------------------------
Path=A:
                    Absolute sector 00000, System BOOT

Displacement ----------------- Hex codes---------------------     ASCII value
 0000(0000)  EB 3E 90 50 43 20 54 6F 6F 6C 73 00 02 02 01 00     > PC Tools
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 00 00     p
 0032(0020)  00 00 00 00 0F 00 00 00 00 01 00 00 00 00 00 00
 0048(0030)  00 00 06 00 01 04 0C 00 00 00 00 00 00 00 00 00
 0064(0040)  FA FC 33 C0 8E D0 BC 00 7C 36 C5 36 78 00 1E 56      3+  = ¦6 6x ^V
 0080(0050)  8E C0 8D 3E 20 7C B9 0B 00 AC 26 80 3D 00 74 03     + > ¦    & = t
 0096(0060)  26 8A 05 AA E2 F3 33 C0 8E D8 A3 7A 00 C7 06 78     &     3+   z   x
 0112(0070)  00 20 7C FB CD 13 73 03 E9 B4 00 8A 2E 30 7C 8A      ¦ = s  +  .0¦
 0128(0080)  0E 32 7C 8A 36 31 7C B2 00 BB 00 05 B8 01 02 CD     2¦ 61¦* =     =
 0144(0090)  13 72 E5 8D 36 62 7D 8B FB B9 0B 00 F3 A6 75 0D     r  6b}       u
 0160(00A0)  BF 20 05 B9 0B 00 F3 A6 74 1A E9 89 00 8D 36 78     +       t     6x
 0176(00B0)  7D 8B FB B9 0B 00 F3 A6 75 7C BF 20 05 B9 0B 00     }       u¦+
 0192(00C0)  F3 A6 75 72 33 D2 A1 1C 05 F7 36 0B 7C FE C0 A2       ur3     6 ¦ +
 0208(00D0)  38 7C BB 00 07 8A 2E 33 7C 8A 0E 35 7C 8A 36 34     8¦=   .3¦  5¦ 64
 0224(00E0)  7C B2 00 A1 18 7C 2A C1 FE C0 50 B4 02 CD 13 58     ¦*  ^¦*  +P+ = X
 0240(00F0)  72 3D 28 06 38 7C 76 1A B4 00 52 F7 26 0B 7C 5A     r=( 8¦v + R & ¦Z

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

รูปที่ 6 เมื่อใช้ View/Edit ดูแผ่นไวรัสที่ผ่านการกำจัดไวรัสแล้วในส่วนบูตเซกเตอร์ จะไม่เห็นข้อความเกี่ยวกับไวรัสอีกต่อไป

```
        data[a+4] = data[a+4]&0xf0;
      else
        {
         data[a] = data[a]&0x0f;
         a++;
        }
      for( b=0;b<4;b++)
         data[a+b] = 0;
      abswrite(0,2,1,data);
      abswrite(0,2,3,data);
      a= b = 5;
      while ( data[a] != 8 && b<11)
          {
            absread(0,1,b,data);
            for( c=0;c<496 ;c++)
              {
                if ((data[c] == 8) && (data[c-2] ==0x6e) && (data[c-5] ==0x72))
                   a = c;
              }
            b++;
          }
       if (b<11)
         {
           b--;
           data[a-1] = data[a-2] = 0x30;
           data[a-9] = data[a-7] = 0x72;
           data[a-10] = data[a-8] =0x69;
           data[a-11] =0x53;
           data[a-6] = 0x61;
           data[a-5] = 0x6a;
           data[a-4] = 0x20;
           data[a-3] = 0x31;
           abswrite(0,1,b,data);
         }
       printf("\nReady! Now diskette in drive A: has a good health.\n");
      }
  }
 else
  printf("\nDiskette in drive A: is quite healthy.\n");
 printf("\n\nDo you want to Search for Virus ? ");
}
printf("\nO.K. QUIT.");
exit();
}
```

– พยายามหลีกเลี่ยงการใช้งานแผ่นที่ไม่เคยได้รับการตรวจหาไวรัส เช่น แผ่นที่ยืมมาใช้งาน เพราะไวรัสอาจติดต่อมายังแผ่นที่ดีได้ หรือก่อนใช้งานให้ทำการตรวจสอบหาไวรัสก่อน ถ้าไม่พบจึงนำมาใช้งาน

– พยายามหลีกเลี่ยงการให้ผู้อื่นยืมไปใช้งาน เพราะอาจติดไวรัสกลับมาได้ หรือตรวจสอบหลังจากให้ผู้อื่นยืมใช้งานทุกครั้ง

– ใช้โปรแกรม สำหรับแก้ไขและตรวจสอบไวรัสในแผ่นจะเป็นวิธีการที่ง่ายที่สุด ดังรูปที่ 4

สรุป

ไวรัสเป็นปรากฏการณ์ใหม่ที่เกิดขึ้นในวงการคอมพิวเตอร์ ซึ่งจะทำให้เกิดความเสียหายและสูญเสียอย่างมากของข้อมูล ทรัพย์สิน เวลา ถ้าหากไม่รีบทำความรู้จักกับมันและทำการป้องกันเสียแต่ตอนนี้ ท้ายนี้ขอให้คุณสนุกกับการตามล่าและกำจัดไวรัสเพื่อความปลอดภัยของข้อมูลของคุณนะครับ